IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,	*	
	*	
v.	*	**Criminal Case No. SAG-24-0120**
	*	
WILLIAM SHEROD, *et al.*	*	
	*	
Defendants.	*	
	*	

* * * * * * * * * * * *

MEMORANDUM OPINION

In this case arising out of a chain of 19 pharmacy burglaries in Maryland, Virginia, and Pennsylvania, three defendants are charged with criminal offenses. At a motions hearing on June 4, 2025, counsel argued a number of motions, two of which the Court reserved for disposition: (1) Defendant William Sherod's motion to suppress evidence obtained pursuant to tower dump warrants, ECF 105; and (2) Sherod's motion to suppress evidence obtained pursuant to the February 26, 2022 warrant, ECF 106. This Court has considered the motions and exhibits, the written opposition filed to the tower dump motion, and Sherod's reply, along with the arguments and exhibits presented at the motions hearing. ECF 108, 123, 128. For the reasons described below, both motions will be denied.

I. FACTUAL BACKGROUND

In the early morning of January 19, 2022, a group of individuals dressed in black, driving a white Honda, committed three separate burglaries of pharmacies in Virginia. Investigators believed the three burglaries were all committed by the same people, in part because each group wore the same clothing, drove the same car, and used the same type of tools. Six days later, Detective Greg Miller of the Harrisonburg (Virginia) Police Department sought and obtained

search warrants from a judge in Rockingham County (Virginia) Circuit Court. ECF 108-2, 108-3. The warrants sought "tower dump" records from AT&T Wireless and T-Mobile for the locations of the three pharmacies for a brief window surrounding each burglary.[1] *Id.* Three days later, investigators sought and obtained an identical warrant for the same records from Verizon Wireless. ECF 108-4. For two of the three burglaries, the warrants sought a thirty-minute window. *Id.* For one burglary, in Charlottesville, VA, the warrants request records from 00:30 am to 2:00 am, a ninety-minute range. *Id.* Each warrant application attested, "Because of the prevalence of cell phones in today's society, there is a strong likelihood that the suspect(s) responsible for the crime was/were in possession of at least one cell phone at the time of the crime." ECF 108-2, 108-3, 108-4. The affidavits conceded that investigators did not know which cell phone provider might have been used by the unknown suspect or suspects. *Id.* The affidavits explained that cellular service providers can also collect information about phones that are not actively being used by otherwise connect to the cellular towers because they are in the radius. *Id.* The tower dump warrants did not request subscriber or other personal identifying information relating to numbers using the cell towers. Instead, they requested only records of communications occurring within the relevant window (incoming and outgoing numbers), records showing the phone numbers that were connected to the cell sites during the relevant time frame but idle[2], and location information showing where the devices were located during the time windows. *Id.* In other words, the warrants authorized investigators to receive information about the location of phone numbers connecting to

[1] A "tower dump" is "a download of information on all the devices that connected to a particular cell site during a particular interval." Wayne R. LaFave, *1 Search & Seizure* § 2.7(f) (6th ed. 2022).

[2] The warrants' request for this type of "idle phone" information (known as "HLR (Home Local Registry) or VLR (Visitor Local Registry) records") contravenes Sherod's contention, apparently based on evidence cited in the 2018 *Carpenter* case, that wireless carriers only retain CSLI data when a call or text occurs. ECF 128 at 9. Obviously, significant technological advances have been made in the years since *Carpenter*.

the cell sites servicing the burglary locations during the relevant windows, but no information tying those numbers to specific people.

Less than a month later, on February 8, 2022, and again in the wee hours of the morning, two pharmacy burglaries occurred in Louisa County, Virginia. Again, a group of suspects in all black clothing, ski masks, and mechanics' gloves used a Halligan bar to force open the pharmacies' doors. This time, the group drove a red Honda Civic. On February 12, 2022, Detective Sergeant Mark Stanton of the Louisa County Sheriff's Office applied for another set of tower dump warrants to serve on Sprint, T-Mobile, and Verizon. ECF 108-5, 108-6, 108-7. These warrants sought records for a 60- or 75-minute window surrounding the locations of the two burglaries. *Id.* The warrants were authorized by Magistrate David Pennington of the Louisa County (Virginia) Circuit Court. *Id.* The affidavits included the statement, "Based on your affiant's training and experience, your affiant is aware people commonly carry cellular telephones and cellular service providers record information about the usage events and subscriber information when those phones are used." *Id.* The warrants requested precisely the same type of information as the warrants sought by Detective Miller in Rockingham County — information about the numbers connecting to the cell sites and their locations, but not any subscriber information identifying the users. *Id.*

On February 26, 2022, Sgt. Stanton used the information he gleaned from his tower dump warrants to apply for a new search warrant requesting more extensive phone records for a single telephone number, (202) 440-3164. ECF 106-1. This time, the information requested included consumer/subscriber information, call detail records, and historical cell site and location information for approximately six weeks. *Id.* The warrant application specified that the 3164 number had been in contact with a cell phone ending in 0022 using the cell sites serving the locations of both Louisa County burglaries on February 8, 2022, within ten minutes of the

respective burglaries at 2:41 am and 4:00 am, and noted that the respective cell towers closest to the two burglaries are approximately 21 miles apart. *Id.*

Finally, on February 28, 2022, Detective Miller sought another series of tower dump warrants, from a different judge in Rockingham County Circuit Court, relating to a third pharmacy burglary that occurred at 1:11 am on February 8, 2022 in Harrisonburg, Virginia (just before the two burglaries investigated by Sergeant Stanton). ECF 108-8, 108-9, 108-10. Like the two burglaries in Louisa County that same night, the suspects drove a red Honda with a sunroof, used a crowbar and Halligan bar to pry open the door, and wore similar clothing. *Id.* The judge approved three tower dump warrants for AT&T, T-Mobile and Verizon, seeking cell site records for a 25-minute window surrounding the burglary. *Id.* The affidavits included the same language as Detective Miller's other affidavits regarding cell phone usage. *Id.*

Additional burglaries occurred throughout February, March, and April, 2022 in Maryland and Pennsylvania. Investigators used physical surveillance, pinging of cellphones, and GPS vehicle trackers to further their investigation, in addition to warrants for additional records using the information gleaned from the tower dumps. Eventually, they apprehended Sherod, Dorman, and co-defendant Deonte Britton while they were committing a pharmacy burglary in Salisbury, Maryland on April 12, 2022.

Sherod contends that the evidence collected pursuant to the tower dump warrants should be suppressed and that the evidence collected pursuant to the February 26, 2022 warrant should be suppressed as well, along with any derivative evidence.

II. LEGAL STANDARDS

As the Supreme Court has instructed, "capacity to claim the protection of the Fourth Amendment depends ... upon whether the person who claims the protection of the Amendment has

a legitimate expectation of privacy in the invaded place." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978); *Rawlings v. Kentucky*, 448 U.S. 98 (1980)). "A subjective expectation of privacy is legitimate if it is one that society is prepared to recognize as reasonable." *Minnesota v. Olson*, 495 U.S. 91, 95–96 (1990). The defendant bears the burden of showing that he has a reasonable expectation of privacy in the area searched. *See Rawlings*, 448 U.S. at 104.

Where the Fourth Amendment is implicated, a search warrant must be supported by probable cause and must particularly describe "the place to be searched, and the persons or things to be seized." *United States v. Drummond*, 925 F.3d 681, 686 (4th Cir. 2019). Probable cause must be based on "more than bare suspicion," *Brinegar v. United States*, 338 U.S. 160, 175 (1949). Courts are to make a "practical, common-sense decision, based on sworn facts, whether there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018).

If a warrant fails to meet those legal standards and a search is unreasonable, the resulting evidence may be subject to suppression. *See United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018) ("The exclusionary rule ordinarily provides that evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure."). But even where the exclusionary rule would otherwise apply, evidence recovered pursuant to a defective warrant is admissible if police had an "objectively reasonable" or "good faith" belief that the warrant was lawful. *United States v. Leon*, 468 U.S. 897 (1984). The *Leon* good faith exception does not apply, and the evidence may still be excluded, where "the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official believe in its existence entirely unreasonable" or "the warrant is so facially deficient — *i.e.*, in failing to

particularize the place to be searched or the things to be seized — that the existing officers cannot reasonably presume it to be valid." *United States v. Doyle*, 650 F.3d 460, 467 (4th Cir. 2011).

III. ANALYSIS

A. Tower Dump Warrants

Sherod argues that the tower dump information gleaned from the three sets of warrants, and any derivative evidence, should be excluded at trial. For the reasons set forth below, this Court concludes that there is no basis to exclude the tower dump information for two reasons: (1) the three sets of tower dump warrants in this case were supported by probable cause; and (2) even if the warrants were deficient, the good faith exception applies.

1. Reasonable Expectation of Privacy

Sherod first asks this Court to determine whether he had a reasonable expectation of privacy in the tower dump records such that a valid search warrant would be required to obtain the information. Specifically, Sherod asks this Court to extend the holding in *Carpenter v. United States*, 585 U.S. 296 (2018), requiring search warrants based on probable cause to obtain the historical cell site location information sought in that case, to tower dump information like that obtained in this investigation.[3] However, because the investigators here sought and obtained search warrants for all of the tower dump records, this Court need not address this preliminary issue, which has been hotly contested in various courts since the Supreme Court left the question open in *Carpenter.* Instead, this Court will focus on whether the search warrants issued in this case were valid and, if not, whether good faith applies.

[3] This question regarding whether the *Carpenter* principles should extend to tower dumps will be appropriate for resolution in a case where tower dump information is obtained via an order pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d).

2. Probable Cause

The three sets of tower dump warrants in this case were supported by probable cause and were sufficiently particularized. Sherod advances a number of challenges to the warrants' content, each of which is unpersuasive for the reasons discussed below.

First, Sherod contests the existence of probable cause to believe that the requested tower dumps would yield evidence of criminal conduct. His attack on the warrants' probable cause encompasses two prongs: 1) the lack of specific evidence that the persons committing these pharmacy burglaries had cell phones on their persons, and 2) the lack of information regarding their use of any specific cellular service provider. On the first point, this Court concludes that the circumstances of these particular crimes (involving multiple participants) and the realities of modern life combine to permit a finding of probable cause that the perpetrators carried cell phones. As the Supreme Court expressly recognized, cell phones "have become 'almost a feature of human anatomy' that individuals 'compulsively carry … with them all the time.'" *Carpenter*, 585 U.S. at 311. A person's likelihood of carrying a cell phone is even greater in circumstances where contact with others is paramount, such as committing a burglary with a group of people where one would need a way to communicate with a lookout or getaway driver.[4] Probable cause is about "fair probability," not certainty, and certain assumptions are allowed to be drawn from practical realities. *Hill v. California*, 401 U.S. 797, 802–804 (1971) (noting that "sufficient probability, not certainty, is the touchstone of reasonableness under the Fourth Amendment."). The affiants on the tower dump warrants swore to the pervasiveness of cell phones in today's society, alleging, for

[4] In his briefing, Sherod contends that a person might not carry one's own cell phone and might proactively use a burner phone when engaging in criminal activity. ECF 128 at 8. But linking robberies together through common burner numbers would still give investigators important evidence about the series of crimes.

example, "[Y]our affiant is aware people commonly carry cellular telephones[.]" and "Because of the prevalence of cell phones in today's society, there is a strong likelihood that the suspects responsible for the crime was/were in possession of at least one cell phone at the time of the crime." As the Fourth Circuit has affirmed in other contexts, issuing judges are not required to check their everyday experiences and common knowledge at the door when evaluating warrant applications. *See, e.g.*, *United States v. Williams*, 548 F.3d 311, 319 (4th Cir. 2008) (noting that even where not "explicitly articulated by the applying officer," the issuing judge could implicitly arrive at the reasonable suspicion "that drug traffickers store drug-related evidence in their homes."). Here, though, the applying officers did expressly remind the issuing judges of the ubiquity of cell phones and the multiple participants in each robbery as they articulated the basis for probable cause.

Sherod's second "probable cause" argument is that because the investigators had no specific information about which cellular service provider each suspect used, each individual warrant lacks a "fair probability" of returning information relevant to the crimes. In other words, because the investigators cannot be sure which warrant within the set of related warrants will bear fruit, they all lack probable cause. While this is a close question and the parties have not pointed the Court to any applicable precedent, this Court believes that the proper analysis would consider each set of tower dump warrants collectively as a unit (as they were presented to the issuing judges), not individually.[5] Put differently, the "place to be searched" is the cell site closest to each pharmacy for the phones making contact with it, not AT&T or T-Mobile or Sprint or Verizon, which are simply the repositories where those records are stored. As the applicants explained to the judges, they did not know which phone company each suspect used, but reasonably believed

[5] Of course, the January 2022 warrants were submitted on two different dates: January 25 for the AT&T and T-Mobile warrants and January 28 for the Verizon warrant. Because all three were submitted to the same judge using the same affidavit, however, they remain a collective set.

there was probable cause that the set of warrants would produce evidence of a crime. In fact, that was the entire point of seeking the information. Requiring an investigator to have probable cause regarding which cellular service provider a suspect is using before the suspect has even been identified would, of course, preclude any such warrant from issuing, even with ample probable cause to believe that the series of warrants would identify the phone(s) the suspect(s) used during the burglaries.

Sherod's other line of attack is on the warrants' particularity. He first contends that the warrants are insufficiently particular because they constitute "all persons warrants" and authorize a search of all persons who used the cell tower, most of whom will have had no connection to the crime. This Court believes this position to be an unwarranted extension of the holdings in *Ybarra v. Illinois*, 444 U.S. 85, 88 (1979) and *Owens ex rel. Owens v. Lott*, 372 F.3d 267 (4th Cir. 2004). In *Ybarra*, police had obtained a warrant to search a tavern and its bartender, but during execution of the warrant, also conducted pat down searches of the individual customers within the tavern. 444 U.S. at 88–89. The Supreme Court ruled that because each person "was clothed with constitutional protection against an unreasonable search or an unreasonable seizure" separate and apart from the protection afforded the tavern's proprietor or the bartender, the search warrant did not authorize the searches of the customers. *Id.* at 91. More broadly, a search warrant does not authorize the search of an unnamed individual unless the warrant specifies that individual or exigent circumstances exist. *Id.* at 91. *Owens* presented a situation where police had sought and obtained a warrant authorizing the search of "all persons" within a private residence that had been connected to drug trafficking. The Fourth Circuit acknowledged a lack of precedent about "[w]hether, and under what circumstances, an 'all persons' warrant is valid under the Fourth Amendment," ultimately concluding that the officers were entitled to qualified immunity because

the law was not specifically clear. 372 F.3d at 274. But the court determined that the information in the affidavit failed "to provide the kind of information that would establish probable cause to believe every person found on the premises was likely involved in the selling and buying of drugs" as would be needed to justify individual searches of their persons. *Id.* at 278.

The flaw in Sherod's contention that this case is the equivalent of an "all persons warrant" is that the searches here (consisting of the acquisition of phone records from third-party phone providers without directly connecting the phone numbers to any user) do not remotely approximate the physical searches of persons in *Ybarra* and *Owens*. Not every search presents the same degree of infringement of privacy rights. For example, the Supreme Court "has long distinguished between an automobile and a home or office" in terms of the degree of intrusiveness of the search. *Chambers v. Maroney*, 399 U.S. 42, 48 (1970). On that sliding scale, the search of a person is highly intrusive. Obtaining targeted phone records from a third-party phone provider is not. These tower dump warrants are not "all persons" warrants because no persons were searched.

While it is beyond dispute that the information collected in the tower dump included phone numbers other than those appearing at multiple burglary sites at the times of the burglaries, Sherod lacks standing to challenge the privacy interests of those unspecified persons. *See United States v. Payner*, 447 U.S. 727, 731 (1980) ("[T]he defendant's Fourth Amendment rights are violated only when the challenged conduct invaded *his* legitimate expectation of privacy rather than that of a third party.") (emphasis in original). Moreover, the limited intrusion into those anonymous persons' privacy interests is not unlike that which happens in other investigative contexts: investigators reviewing surveillance camera footage from a commercial robbery are likely to view others on the footage who were going about their ordinary business. Detectives collecting fingerprints at a bank teller window will likely collect (and possibly even identify) fingerprints

belonging to innocent bank customers. Officers effecting a search of a multiple-resident house or apartment are likely to search the belongings of uninvolved occupants along with those of the suspected perpetrator of the crime. The mere fact of limited intrusion on the privacy interests of innocent persons while executing a valid warrant targeting a viable suspect does not invalidate the warrant or permit one person to assert another's Fourth Amendment claim.

Finally, Sherod argues that these warrants are overbroad because they do not restrict, in any manner, the investigators' use of the data they received regarding persons other than those involved in the crimes. Again, Sherod lacks standing to advance that argument in support of other persons. *See, e.g.*, *Alderman v. United States*, 394 U.S. 165, 174 (1969) ("Fourth Amendment rights are personal rights which … may not be vicariously asserted."). With respect to Sherod's own 3164 number, which appeared at multiple burglary locations, the investigators sought and obtained further warrants to make use of that information. In other words, they essentially employed a two-step process: figure out which numbers connected with multiple cell sites, and then obtain new search warrants to get more information (including subscriber information) for those numbers. But Sherod lacks standing to advance an argument with respect to the collection and potential use of other people's anonymized data.

It is true that these warrants, while reasonably particular in terms of their limited time frames and specified tower locations, did not contain procedures to further restrict the investigators' use of the collected CSLI. For example, the warrants did not include protocols or a multi-step process to allow the phone companies to produce only those the numbers that appeared on multiple cell towers, or to require law enforcement only to retain such numbers and to discard the rest. The overlap of two or more locations would clearly contribute to tying the search results to the fair probability of criminal activity. However, while such restrictions constitute a best

practice, this Court does not deem the absence of such restrictions to be inherently fatal to the particularity requirement of the warrant. Ultimately, this Court finds these tower dump warrants to be sufficiently particular in light of their limited scope and intrusiveness. *See Michigan v. Tyler*, 436 U.S. 499, 506 (1978) ("The showing of probable cause necessary to secure a warrant may vary with the object and intrusiveness of the search, but the necessity of for the warrant persists.").

3. Good Faith

Even if one or more warrants was lacking in probable cause or particularity for one of the reasons discussed above, the good faith exception applies. Tower dumps have been a relatively prevalent investigative technique since cell phone usage became widespread, especially in cases involving multiple connected criminal incidents. Judges regularly sign such warrants and judicial officers approved each of the warrants in this case. There is no clear judicial guidance, at least in the Fourth Circuit, regarding the propriety of tower dump warrants or the requirement to include particular protocols. In fact, jurisprudence in the entire area of cell phone and GPS-based surveillance is rapidly evolving. The disparate court decisions in this arena highlight the difficulty in applying traditional Fourth Amendment principles to modern-day technological advances.[6]

[6] The cases Sherod relies on for his propositions that tower dumps invade reasonable expectations of privacy, require particular protocols, or are otherwise impermissible are nonbinding, out-of-district cases mostly decided *after* the investigators obtained the tower dump warrants in this case. *See, e.g.*, *Matter of Tower Dump Data for Sex Trafficking Investigation*, 2023 WL 1779775 (N.D. Ill. Feb. 6, 2023) (magistrate judge in Northern District of Illinois finding that a warrant is required for tower dumps and that protocols are required to establish particularity); *In re Four Applications for Search Warrants Seeking Info. Associated with Particular Cellular Towers*, 2025 WL 603000 (S.D. Miss. Feb. 21, 2025) (finding that tower dumps are "general, exploratory rummaging" such that the warrants cannot issue). There appear to be like numbers of nonbinding or out-of-circuit cases ruling in the opposite direction, including recent cases finding that search warrants are not required because tower dump records can be obtained with § 2703(d) orders alone. *See, e.g.*, *United States v. Pricop*, 2025 WL 918337, at *3 (D. Ariz. Mar. 26, 2025) (ruling that tower dumps are "different from the continuous monitoring of a single person's location for multiple days at issue in *Carpenter*"); *United States v. Williams*, 741 F. Supp. 3d 642, 649 (E.D. Mich. 2024) (permitting such records to be obtained by § 2703(d) order because it requires only "reasonable grounds to

The exclusionary rule is not "designed to redress the injury occasioned by an unconstitutional search" *Davis v. United States*, 564 U.S. 229, 236–37 (2011). Instead, it is designed to serve as a deterrent to improper law enforcement action and is applied only where suppression of the evidence in a given case would produce a deterrent effect in future cases. *Leon*, 468 U.S. at 909. Where, as here, a defendant contends "that a search warrant contained grossly insufficient information," the Fourth Circuit counsels that it "is best analyzed under the third *Leon* exception." *United States v. Wellman*, 663 F.3d 224, 229 (4th Cir. 2011). In other words, this Court must consider whether the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *Doyle*, 650 F.3d at 467, or "so obviously deficient" in particularity as to constitute a "general warrant." *Groh v. Ramirez*, 540 U.S. 551, 558, 561 (2004).

This Court cannot make those findings on these facts. Three different judges found that these very similar warrants contained probable cause and were sufficiently particular to justify their issuance. The investigators would have no reason to believe that the judges would issue grossly deficient warrants. At this point, no binding precedent suggests that these sort of warrants were illegal. In fact, the arguments advanced by Sherod require "a detailed, nuanced understanding and application of Fourth Amendment principles, which police officers are not and cannot be expected to possess." *United States v. Chatrie*, 590 F.Supp.3d 901 (2022), *aff'd* by *United States v. Chatrie*, 136 F.4th 100 (4th Cir. 2025) (en banc).[7] The Court cannot say, in these circumstances,

---

believe" that tower dump records are "relevant and material" to the ongoing investigation); *United States v. Walker*, 2020 WL 4065980, at *23 (E.D.N.C. Jul. 20, 2020) ("In light of the significant differences between a tower dump CSLI and long term CSLI targeted at the whole of an individual's movements, as highlighted by the court's decision in *Carpenter*, the court finds no basis for attaching a Fourth Amendment interest to tower dump CSLI.").

[7] The *Chatrie* case exemplifies the complexity in these legal questions and the vast room for dissent in the application of accepted legal principles to new technologies. The case weighed the use of

that the investigators' reliance on the three sets of tower dump warrants issued by three state judicial officers was objectively unreasonable or that exclusion of the tower dump evidence in this case would "meaningfully deter" improper law enforcement conduct in subsequent investigations. *Herring v. United States*, 555 U.S. 135, 144 (2009).

B. February 26 Warrant

In addition to his futile argument that the February 26 warrant application is invalid because it derives from the tower dump information, Sherod makes three alternative arguments. He argues: (1) that the issuing judge had no basis to conclude the suspects were using cell phones during the burglary; (2) that the issuing judge had no basis to conclude that the suspects were even carrying cell phones during the burglary; and (3) that the warrant provided no nexus between the requested records for the 3164 phone and the burglary suspects.

This Court disagrees. The February 26 affidavit specifies that multiple suspects were involved in each robbery and asserts the common-sense proposition that, "It is likely that the suspect(s) being from out of the area are using their cell phones for navigation purposes and communications with other members of their group." ECF 108-11. For all the reasons described

---

Google's location data, and a process known as geofencing, to identify a bank robbery suspect. To overly simplify the court's complex analysis, the district judge concluded that the use of the geofence data constituted a search, that the warrant lacked probable cause because it needed to have probable cause as to each phone implicated in the geofence, and that the good faith exception applied because the legal issues were novel. *Chatrie*, 590 F. Supp. 3d 901. In an *en banc* review of the case at the Fourth Circuit, the judges were so divided that the court could muster only a one-line *per curiam* opinion stating, "[T]he judgment of the district court is AFFIRMED." *Chatrie*, 136 F.4th at 100. As Chief Judge Diaz summarized in his concurrence, "My colleagues have widely divergent views on the intersection of the Fourth Amendment and the groundbreaking investigative tool at issue here." *Id.* at 101. The remainder of the voluminous decision consists only of a multitude of concurrences and dissents advancing those widely divergent views, ultimately reflecting that approximately nine of the judges agreed with the district court that the good faith exception applied. Of course, that resolution provides little guidance to district courts considering similar disputes or to investigators seeking to comport their actions with the law.

above, the issuing judge had a fair probability based on the facts, modern-day realities, and common sense to believe that the suspects would be using and carrying cell phones as they worked collectively to accomplish their crimes. And the nexus between the 3164 number and the robberies is established by the fact that the tower dump information showed that both the 3164 number and a phone ending in 0022 made contact with the cell towers in the vicinity of two separate robberies in the wee hours of the morning, 21 miles from one another. *Id.* The judge was presented with a fair probability that the phone had been involved in criminal activity, as it would have to be an exceptional coincidence for two phones unrelated to the burglaries to have traveled to those specific two distant locations between 2 and 4 a.m. on the same night and at the same time the two burglaries occurred.

Finally, the *Leon* good faith exception would apply to this warrant as well, which was signed by a neutral and detached state court judge. Sherod has made no showing to invoke any of the limited *Leon* exceptions and demonstrate why future misconduct would be deterred by the exclusion of the phone record evidence.

IV. CONCLUSION

For the reasons set forth above, Sherod's two motions to suppress, ECF 105 and 106, will be DENIED.

Date: June 23, 2025

/s/
Stephanie A. Gallagher
United States District Judge